REMARKS

Reconsideration of the above referenced application in view of the enclosed amendments and remarks is requested. Claims 1, 4, 7, 8, 11, 21, and 23 have been amended. Claims 2, 3, 5, 9, 10, and 12-20 have been canceled. New claims 24-31 have been added. Claims 1, 4, 6-8, 11, and 21-31 remain in the application.

ARGUMENT

Claims 1-4, 8-11, 13, 17-18, and 20-21 are rejected under 35 USC 103(a) as being unpatentable over Perlman, et al. (US 5,978,381) (hereinafter Perlman) in view of Roberts, et al. (US 6,920,110)(hereinafter Roberts).

The present invention relates to protecting content in a client-server system wherein a server broadcasts or multicasts content to many client devices. For example, the client device may be a set-top box for receiving TV programming or PPV movies over a cable TV or satellite TV system. An operator of the server may attempt to protect access to the content by designing the client device software such that it is tamper resistant according to known methods. Despite this, it still may be possible for malicious users to circumvent the tamper-resistant software and modify the client device's billing log so that the log shows little or no client device activity. For example, it may be possible for a hacker to change the actual viewing history recorded in the billing log so that the hacker is billed less money (or even no money) by the server operator. If the billing log is modified in this manner, the operator of the server will lose revenue.

One approach to deterring such activity would be to uniformly update the software on all client devices periodically. The new software may contain new cryptographic or tamper resistant techniques to thwart any would-be hackers. However, when the number of client devices is very large (i.e., millions of devices), this is impractical due to the load on the communications network. Another approach would be to update only those client devices where it may be detected

that the billing log has been tampered with. However, such detection is very difficult, if not impossible. Hence, a method of selectively updating only certain client devices regardless of detectability of hacking activity or the number of client devices would be useful to server operators.

Thus, embodiments of the present invention comprise a system and method wherein the server periodically obtains billing log data from the client devices, and maintains a billing database or a portion of a billing database for each client device. The billing database stores billing log data obtained from the client device. The billing database comprises the content consumption activity of the client device for a selected period of time. If the billing log data for a given client device indicates consumption of PPV audio-visual content that is *less than* a predetermined threshold for the selected period of time, then the client device may be marked in the billing database as eligible to receive a software update. *In this way, reported client activity is used to determine when new software updates should be performed, because if the activity is too low, it is assumed that the billing log on the client device has been hacked.* By targeting only those client devices that are not reporting much, if any, content reception and consumption activity, the overall time spent downloading new software to client devices may be reduced and the overall bandwidth required to distribute software updates may be reduced.

Turning now to the cited prior art, Perlman discloses the WebTV system where web pages from web sites that a user is interested in are downloaded during off-peak hours to the client device. In Perlman's system, the criteria for determining what web pages to download at off-peak times is whether the user has viewed web pages from a particular web site. Perlman's reference to "usage patterns" refers to the web sites that the user has visited. The data uploaded from Perlman's client device (e.g., a PC) to the WebTV server is the list of addresses (URLs) of content to be downloaded to the user device at off-peak times. This is not billing log data.

Roberts discloses the well known "Windows Update" feature of Microsoft Windows. Windows Update measures the bandwidth being currently used for the communications channel of a user's Internet session and determines how much Windows update software portions to download to the user's machine per unit time

so as to not overload the user's current session. The update software download runs "in the background" in a way that does not significantly interfere with the user's current on-line tasks. To do this, the server measures the user's *current* on-line activity (e.g., web browsing, e-mail, etc.), not past user downloads of content.

Turning now to independent claim 1, it has been amended to more particularly recite the present invention. Claim 1 now recites that billing log data is received, the billing log data specifying past consumption of pay-per-view (PPV) audio-visual content received by the client device from a server over a broadcast network during a selected period of time. Further, claim 1 recites downloading an update for the software resident on the client device from the server, the software, when executing on the client device, for decrypting the PPV audio-visual content and controlling consumption of the PPV audio-visual content, the downloading being performed when the received billing log data indicates past consumption of PPV audio-visual content by the client device at less than a predetermined threshold for the selected period of time.

Perlman does not teach or suggest that *billing log data* specifying *past consumption of PPV audio-visual content* is received by the server. Roberts does not teach or suggest that *past consumption activity by the client device of PPV audio-visual content is reviewed* to determine whether a new software update should be downloaded to the client device.

Neither Perlman nor Roberts, alone or in combination, teach or suggest that *the level of past consumption of PPV audio-visual content by a client device as described in billing log data is used to determine whether to update client device software for decrypting and consuming the PPV audio-visual content, as currently claimed.* Furthermore, neither of the cited references teach or suggest that falling below a threshold level of past consumption of PPV audio-visual content will trigger an update to the client device's software.

Since neither Perlman, nor Roberts, either alone or in combination, teach or suggest the claimed limitation, independent claim 1 is allowable as presented.

Claims 4, 6, and 7 depend from allowable independent claim 1. Hence, they are also allowable.

New claims 24-27 are also dependent on claim 1, so they are also allowable.

For independent claim 8, a similar rationale as stated above is applicable. Therefore, claim 8 is also allowable. Additionally, claim 11 is allowable since it is dependent from allowable claim 8.

As to independent claim 21, it contains similar limitations as allowable independent claim 1. Therefore, it is also allowable under the same rationale. In addition, it is clear from a reading of claim 21 that it requires at least three elements:

1) a billing database to store billing log data received from a plurality of client devices, the billing log data specifying past consumption of pay-per-view (PPV) audio-visual content received by a client device from the server over a broadcast network of the content distribution system during a selected period of time;

2) a client software update database to store versions of updateable content reception and consumption software, the software, when executing on the client device, for decrypting the PPV audio-visual content and controlling consumption of the PPV audio-visual content; and

3) a client software manager configured to receive billing log data from the client devices, to update the billing database using the received billing log data, to mark a client device in the billing database as eligible for receiving updated content reception and consumption software when billing log data for the client device indicates consumption of PPV audio-visual content by the client device at less than a predetermined threshold for the selected period of time, and to download a version of the updateable content reception and consumption software to each marked client device for subsequent use in receiving, decrypting, and consuming content.

The Applicants do not see where the claimed billing database, the claimed client software update database, and the claimed client software manager are taught or suggested in Perlman or Roberts. These are structural elements that are not in claim 1, and cannot be rejected based on a conclusory reference to claim 1. Simple references to usage patterns are not enough evidence to make out a prima facie case of obviousness for these claim elements that will stand up on appeal to

the Board. Clarification is respectfully requested. Without more, the Examiner has not fulfilled the Examiner's burden for rejecting this claim.

New claims 28-31 are dependent on allowable independent claim 21. Thus, they are also allowable.

Claims 5-7, 12, 14-16, 19, and 22-23 are rejected under 35 USC 103(a) as being unpatentable over Perlman in view of Roberts, and further in view of Tsukamoto, et al. (US 5,796,828)(hereinafter Tsukamoto).

Claims 5, 12, 14-16, and 19 are cancelled. Therefore, the rejections of these claims are moot.

Claims 6 and 7 are allowable because they depend from allowable independent claim 1. Further, as to claim 6, the Office action dated June 1, 2006 asserts that Tsukamoto discloses tamper resistance software. This is a factual error on the part of the Examiner. Tsukamoto does not teach or suggest anything about tamper resistance software, as that term is understood by those skilled in the art of security software.

Claims 22 and 23 are allowable because they depend from allowable independent claim 21. Further, as to claim 22, the Office action dated June 1, 2006 asserts that Tsukamoto discloses tamper resistance software. This is a factual error on the part of the Examiner. Tsukamoto does not teach or suggest anything about tamper resistance software, as that term is understood by those skilled in the art of security software.

CONCLUSION

In view of the foregoing, Claims 1, 4, 6-8, 11, and 21-31 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (503) 264-8074. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

/Steven P. Skabrat/
Steven P. Skabrat
Registration No. 36,279
Senior Attorney
Intel Corporation
(503) 264-8074

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026